What is claimed is:

1. A system for managing files comprising a computer and a storage unit, wherein

the computer comprises

reciprocal authenticating means for reciprocally authenticating the computer with the storage unit and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys;

access allowing key storing means for storing the access allowing keys; and

file accessing means for sending an access request together with the access allowing key, and

the storage unit comprises

reciprocal authenticating means for reciprocally authenticating the storage unit with the computer and when the computer and the storage unit are authenticated with each other, creating access allowing keys;

access allowing key group storing means for storing all the access allowing keys;

access allowing key identification means for identifying if the access allowing key sent from the file accessing means and stored in the access allowing key storing means and at least one access allowing key stored in the access allowing key group storing means, are the same; and

secure area accessing means for accessing a secure area usually unaccessible.

2. The system for managing files according to claim 1, wherein the reciprocal authenticating means provided in said computer and said file accessing means are implemented by a unit of hardware.

3. A system for managing files, comprising:

sub-file storing means for storing one or a plurality of sub-files related to a main-file;

authentication information creating means for creating sub-file authentication information used to verify the sub-files; and

system file storing means for storing a system file to which the sub-file authentication information is related.

4. A system for managing files, comprising:

main-file storing means for storing a main-file;

authentication information creating means for creating main-file authentication information to be used to verify the main-file; and

sub-file storing means for storing at least one sub-file to which the main-file authentication information is related.

5. A system for managing files, comprising:

main-file storing means for storing a main-file;

sub-file storing means for storing at least one sub-file to which the main-file authentication information is related;

authentication information creating means for creating main-file authentication information to be used to verify the main-file/sub-file authentication information to be used to verify the sub-files; and

system file storing means for storing a system file to which the sub-file authentication information is related.

6. The system for managing files according to claim 5, wherein said main-file, said sub-files and said system files are stored in a non-secure area usually accessible.

7. The system for managing files according to claim 5, wherein said main-file, and said sub-files and said

system files are stored in a non-secure area usually accessible and a secure area usually unaccessible, respectively.

8. The system for managing files according to claim 5, wherein said main-file and said sub-files, and said system files are stored in a non-secure area usually accessible and a secure area usually unaccessible, respectively.

9. The system for managing files according to claim 6, further comprising a computer and a storage unit, wherein

the computer comprises

reciprocal authenticating means for reciprocally authenticating the computer with the storage unit and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys;

access allowing key storing means for storing the access allowing keys; and

file accessing means for sending an access request together with the access allowing key,

the storage unit comprises

reciprocal authenticating means for reciprocally authenticating the storage unit with the computer and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys;

access allowing key group storing means for storing all the access allowing keys; and

access allowing key identification means for identifying if the access allowing key sent from the file accessing means and stored in the access allowing key storing means and at least one access allowing key stored in the access allowing key group storing means, are the same; and

secure area accessing means for accessing a secure area usually unaccessible, and

the authentication information creating means reads a medium ID peculiar to the medium stored in the secure area, and uses the medium ID to create the main-file authentication information and the sub-file authentication information after the computer and the storage unit are reciprocally authenticated.

10. The system for managing files according to claim 7, further comprising a computer and a storage unit, wherein

the computer comprises

reciprocal authenticating means for reciprocally authenticating the computer with the storage unit and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys;

access allowing key storing means for storing all the access allowing keys; and

file accessing means for sending an access request together with the access allowing key,

the storage unit comprises

reciprocal authenticating means for reciprocally authenticating the storage unit with the computer and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys;

access allowing key group storing means for storing all the access allowing keys; and

access allowing key identification means for identifying if the access allowing key sent from the file accessing means and stored in the access allowing key storing means and at least one access allowing key stored in the access allowing key group storing means, are the same; and

secure area accessing means for accessing a secure area usually unaccessible, and the authentication information creating means reads a medium ID peculiar to the medium stored in the secure area, and uses the medium ID to create the main-file authentication information and the sub-file authentication information after the computer and the storage unit are reciprocally authenticated.

11. The system for managing files according to claim 8, further comprising a computer and a storage unit, wherein

the computer comprises

reciprocal authenticating means for reciprocally authenticating the computer with the storing unit and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys;

access allowing key storing means for storing the access allowing key; and

file accessing means for sending an access request together with the access allowing key,

the storage unit comprises

reciprocal authenticating means for reciprocally authenticating the storage unit with the computer and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys;

access allowing key group storing means for storing all the access allowing keys; and

access allowing key identification means for identifying if the access allowing key sent from the file accessing means and stored in the access allowing key storing means and at least one access allowing key stored in the access allowing key group storing means, are the same; and

secure area accessing means for accessing a secure area usually unaccessible, and

the authentication information creating means reads a medium ID peculiar to the medium stored in the secure area, and uses the medium ID to create the main-file authentication information and the sub-file authentication information after the computer and the storage unit are reciprocally authenticated.

12. The system for managing files according to claim 9, wherein

the reciprocal authenticating means provided in said computer and said file accessing means are implemented by means of hardware.

13. The system for managing files according to claim

9, wherein

the medium ID is a card ID.

14. The system for managing files according to claim 9, wherein

the medium ID is a master ID.

15. The system for managing files according to claim 9, wherein

said authentication information is created for each record of a file.

16. The system for managing files according to claim 10, wherein

said authentication information is created for each record of a file.

17. The system for managing files according to claim 11, wherein

said authentication information is created for each record of a file.

18. A system for managing files, comprising:

sub-file reading means for reading one or a plurality of sub-files related to a main-file;

authentication information creating means for creating sub-file authentication information from sub-files read by the sub-file reading means;

system file reading means for reading sub-file authentication information from a system file related to the sub-file; and

authentication information comparing means for comparing the sub-file authentication information created by the authentication information creating means with the sub-file authentication information read by the system file reading means.

19. A system for managing files, comprising:

main-file reading means for reading a main-file;

authentication information creating means for creating main-file authentication information from a main-file read by the main-file reading means;

sub-file reading means for reading main-file authentication information from sub-files related to the main-file; and

authentication information comparing means for comparing the main-file authentication information created by the authentication information creating means with the main-file authentication information read by the sub-file reading means.

20. A system for managing files, comprising:

main-file reading means for reading a main-file;

sub-file reading means for reading main-file authentication information from sub-files related to the main-file and one or a plurality of sub-files related to the main-file;

system file reading means for reading sub-file authentication information from a system file related to the sub-file;

authentication information creating means for creating main-file authentication information from a main-file read by the main-file reading means and creating sub-file authentication information from sub-files read by the sub-file reading means; and

an authentication information comparing means for comparing the main-file authentication information created by the authentication information creating means with the main-file authentication information read by the sub-file reading means and comparing the sub-file authentication information created by the authentication information creating means with the sub-file authentication information read by the system file reading means.

21. The system for managing files according to claim

20, wherein said main-file, said sub-files and said system file are stored in a non-secure area usually accessible.

22. The system for managing files according to claim 20, wherein said main-file, and said sub-files and said system file are stored in a non-secure area usually accessible and a secure area usually unaccessible, respectively.

23. The system for managing files according to claim 20, wherein said main-file and said sub-files, and said system file are stored in a non-secure area usually accessible and a secure area usually unaccessible, respectively.

24. The system for managing files according to claim 21, further comprising a computer and a storage unit, wherein

the computer comprises

reciprocal authenticating means for reciprocally authenticating the computer with the storing unit and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys;

access allowing key storing means for storing the access allowing keys; and

file accessing means for sending an access request together with the access allowing key,

the storage unit comprises

reciprocal authenticating means for reciprocally authenticating the storage unit with the computer and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys;

access allowing key group storing means for storing all the access allowing keys; and

access allowing key identification means for identifying if the access allowing key sent from the file accessing means and stored in the access allowing key storing means and at least one access allowing key stored in the access allowing key group storing means, are the same; and

secure area accessing means for accessing a secure area usually unaccessible, and

the authentication information creating means reads a medium ID peculiar to the medium stored in the secure area, and uses the medium ID to create the main-file authentication information and the sub-file authentication information after the computer and the storage unit are reciprocally authenticated.

25. The system for managing files according to claim 22, further comprising a computer and a storage unit, wherein

the computer comprises

reciprocal authenticating means for reciprocally authenticating the computer with the storing unit and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys;

access allowing key storing means for storing the access allowing key; and

file accessing means for sending an access request together with the access allowing key,

the storage unit comprises

reciprocal authenticating means for reciprocally authenticating the storage unit with the computer and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys;

access allowing key group storing means for storing all the access allowing keys; and

access allowing key identification means for identifying if the access allowing key sent from the file accessing means and stored in the access allowing key storing means and at least one access allowing key stored in the access allowing key group storing means, are the same; and

secure area accessing means for accessing a secure area usually unaccessible, and

the authentication information creating means reads a medium ID peculiar to the medium stored in the secure area, and uses the medium ID to create the main-file authentication information and the sub-file authentication information after the computer and the storage unit are reciprocally authenticated.

26. The system for managing files according to claim 23, further comprising a computer and a storage unit, wherein

the computer comprises

reciprocal authenticating means for reciprocally authenticating the computer with the storing unit and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys;

access allowing key storing means for storing all the access allowing keys; and

file accessing means for sending an access request together with the access allowing key,

the storage unit comprises

reciprocal authenticating means for reciprocally authenticating the storage unit with the computer and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys;

access allowing key group storing means for storing all the access allowing keys; and

access allowing key identification means for identifying if the access allowing key sent from the file accessing means and stored in the access allowing key storing means and at least one access allowing key stored in the access allowing key group storing means, are the same; and

secure area accessing means for accessing a secure area usually unaccessible, and

the authentication information creating means reads a medium ID peculiar to the medium stored in the secure area, and uses the medium ID to create the main-file authentication information and the sub-file authentication information after the computer and the storage unit are reciprocally authenticated.

27. The system for managing files according to claim

24, wherein

the reciprocal authenticating means provided in said computer and said file accessing means are implemented by means of hardware.

28. The system for managing files according to claim 24, wherein

the medium ID is a card ID.

29. The system for managing files according to claim 24, wherein

the medium ID is a master ID.

30. The system for managing files according to claim 24, wherein

said authentication information is created for each record of a file.

31. The system for managing files according to claim 1, wherein

said secure area accessing means further comprises

access control information reading means for reading access control information stored in said secure area, and said storage unit further comprises

sector accessing means for accessing a main- file or sub-files related to the main-file in units of sectors or sector groups according to the access control information.

32. The system for managing files according to claim 31, wherein

said secure area accessing means further comprises

access control information setting means for setting access control information in said secure area.

33. The system for managing files according to claim 9, wherein

authentication information is created using one, two or all of said medium ID, said card ID and said master ID.

34. The system for managing files according to claim 24, wherein

authentication information is created using one, two or all of said medium ID, said card ID and said master ID.

35. A computer, comprising:

reciprocal authenticating means for reciprocally authenticating the computer with a storing unit and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys; and

access allowing key storing means for storing the access allowing keys; and

file accessing means for sending an access request together with the access allowing key.

36. A storage unit, comprising:

reciprocal authenticating means for reciprocally authenticating the storage unit with a computer and when the computer and the storage unit are authenticated with each other, creating access allowing keys;

access allowing key group storing means for storing all the access allowing keys;

access allowing key identification means for identifying if the access allowing key stored in the access allowing key storing means and at least one access allowing key stored in the access allowing key group storing means, are the same; and

secure area accessing means for accessing a secure area usually unaccessible.

37. A method of managing files, comprising the steps of:

reciprocally authenticating between a computer and a storage unit and when the computer and the storage unit are reciprocally authenticated, creating an access allowing key;

storing the access allowing key;

storing all the access allowing keys;

sending an access request together with the access allowing key;

identifying if the access allowing key stored in the access allowing key storing step and at least one access allowing key stored in the access allowing key group storing step, are the same; and

accessing a secure area usually unaccessible.

38. A method of managing files, comprising the steps of:

storing one or a plurality of sub-files related to a main-file;

creating sub-file authentication information used to verify the sub-files; and

storing a system file to which the sub-file authentication information is related.

39. A method of managing files, comprising the steps of:

storing a main-file;

creating main-file authentication information to be used to verify the main-file; and

storing at least one sub-file to which the main-file authentication information is related.

40. A method of managing files, comprising the steps of:

storing a main-file;

storing at least one sub-file to which the main-file authentication information is related;

creating main-file authentication information to be used to verify the main-file/sub-file authentication information to be used to verify the sub-files; and

storing a system file to which the sub-file authentication information is related.

41. A method of managing files, comprising the steps of:

reading one or a plurality of sub-files related to a main-file;

creating sub-file authentication information from sub-files;

reading sub-file authentication information from a system file related to the sub-file; and

comparing the sub-file authentication information from the sub-files with the sub-file authentication information from the system file.

42. A method of managing files, comprising the steps of:

reading a main-file;

creating main-file authentication information from the main-file;

reading main-file authentication information from sub-files related to the main-file; and

comparing the main-file authentication information from the main-file with the main-file authentication information from the sub-file.

43. A method of managing files, comprising the steps of:

reading a main-file;

reading main-file authentication information from sub-files related to the main-file and one or a plurality of sub-files related to the main-file;

reading sub-file authentication information from a system file related to the sub-file;

creating main-file authentication information from a main-file and creating sub-file authentication information from sub-files; and

comparing the main-file authentication information from the sub-file with the main-file authentication information from the main-file and comparing the sub-file authentication information from the system file with the sub-file authentication information from the sub-file.

44. A method of managing files, comprising the steps of:

reciprocally authenticating a computer with a storing unit and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys; and

storing the access allowing keys; and

sending an access request together with the access allowing key.

45. A method of managing files, comprising the steps of:

reciprocally authenticating a storage unit with a computer and when the computer and the storage unit are authenticated with each other, creating access allowing keys;

storing all the access allowing keys;

identifying if the access allowing key and at least one access allowing key, are the same; and

accessing a secure area usually unaccessible.

46. A computer readable storage medium having a recorded file management program for enabling a computer to execute:

a reciprocal authenticating step of reciprocally authenticating between a computer and a storage unit and when the computer and the storage unit are reciprocally authenticated, creating an access allowing key;

an access allowing key storing step of storing the access allowing key;

an access allowing key group storing step of storing all the access allowing keys;

a file accessing step of sending an access request together with the access allowing key;

an access allowing key identifying step of identifying if the access allowing key stored in the access allowing key storing process and at least one access allowing key stored in the access allowing key group storing step, are the same; and

a secure area accessing step of accessing a secure area usually unaccessible.

47. A computer readable storage medium having a recorded file management program for enabling a computer to execute:

sub-file storing step of storing one or a plurality of sub-files related to a main-file;

authentication information creating step of creating sub-file authentication information used to verify the sub-files; and

system file storing step of storing a system file to which the sub-file authentication information is related.

48. A computer readable storage medium having a recorded file management program for enabling a computer to execute:

main-file storing step of storing a main-file;

authentication information creating step of creating main-file authentication information to be used to verify the main-file; and sub-file storing step of storing at least one sub-file to which the main-file authentication information is related.

49. A computer readable storage medium having a recorded file management program for enabling a computer to execute:

main-file storing step of storing a main-file;

sub-file storing step of storing at least one sub-file to which the main-file authentication information is related;

authentication information creating step of creating main-file authentication information to be used to verify the main-file/sub-file authentication information to be used to verify the sub-files; and

system file storing step of storing a system file to which the sub-file authentication information is related.

50. A computer readable storage medium having a recorded file management program for enabling a computer to execute:

sub-file reading step of reading one or a plurality of sub-files related to a main-file;

authentication information creating step of creating sub-file authentication information from sub-files;

system file reading step of reading sub-file authentication information from a system file related to the sub-file; and

authentication information comparing step of comparing the sub-file authentication information from the sub-file with the sub-file authentication information from the system file.

51. A computer readable storage medium having a recorded file management program for enabling a computer to execute:

main-file reading step of reading a main-file;

authentication information creating step of creating main-file authentication information from a main-file;

sub-file reading step of reading main-file authentication information from sub-files related to the main-file; and

authentication information comparing step of comparing the main-file authentication information from the main-file with the main-file authentication information from the sub-file.

52. A computer readable storage medium having a recorded file management program for enabling a computer to execute:

main-file reading step of reading a main-file;

sub-file reading step of reading main-file authentication information from sub-files related to the main-file and one or a plurality of sub-files related to the main-file;

system file reading step of reading sub-file authentication information from a system file related to the sub-file;

authentication information creating step of creating main-file authentication information from a main-file and creating sub-file authentication information from sub-files; and

authentication information comparing step of comparing the main-file authentication information from the sub-file with the main-file authentication information from the main-file and comparing the sub-file authentication information from the sub-file with the sub-file authentication information from the main-file.

53. A computer readable storage medium having a recorded file management program for enabling a

computer to execute:

reciprocal authenticating step of reciprocally authenticating a computer with a storing unit and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys; and

access allowing key storing step of storing the access allowing keys; and

file accessing step of sending an access request together with the access allowing key.

54. A computer readable storage medium having a recorded file management program for enabling a computer to execute:

reciprocal authenticating step of reciprocally authenticating a storage unit with a computer and when the computer and the storage unit are authenticated with each other, creating access allowing keys;

access allowing key group storing step of storing all the access allowing keys;

access allowing key identification step of identifying if the access allowing key and at least one access allowing key, are the same; and

secure area accessing step of accessing a secure area usually unaccessible.